Frequently Asked Questions

The current version of the HPE Fortify SCA software is 16.20 and the current version of the rulepacks is 2016.4
Announcements such as new HPE Fortify SCA software and rulepack releases are posted HERE

This page has been made public for vendors
> How do I request tools, reviews (validations), or technical support?

To request tools, reviews (validations), or technical support, instructions are below.

STEP 1

Register a custom-developed application HERE

You can check if your application is already registered HERE (Internal Link)

STEP 2

For **secure code review**, request VA licenses for Fortify software HERE,

For **secure design review**, request an initial application threat model HERE

STEP 3

For **secure code review**, request a code review validation HERE

For **secure design review**, request a design review validation HERE

To request training and technical support:

Request Self-Paced **VA Fortify End User Training** Materials HERE

Request Self-Paced **VA Secure Coding Training** Materials HERE

HELP Request **Fortify support**, or e.g. V&V support telecoms HERE ; please also use this link for requests such as:

- To request access to VA secure code review upload/report directories
- To subscribe to the VA Software Assurance Newsletter or
- To check whether a user has already been provisioned the VA-licensed Fortify software

VA | U.S. Department of Veterans Affairs
Office of Information and Technology
Software Assurance Program Office

- Fortify Rulepacks Version 2016.4 Released
  Mike Boberski 12 19, 2016
  OIS Software Assurance
- Fortify Software Version 16.20 Released
  Mike Boberski 12 18, 2016
  OIS Software Assurance
- Microsoft Threat Modeling Tool Now In TRM
  Mike Boberski 11 15, 2016
  OIS Software Assurance
- Fortify Rulepack Version 2016.3.0 Released
  Mike Boberski 10 04, 2016
  OIS Software Assurance
- Upcoming VA Software Assurance Working Group Meetings
  Mike Boberski 9 27, 2016
  OIS Software Assurance
- Self-Paced VA Secure Coding Training Materials Are Now Available
  Mike Boberski 9 26, 2016
  OIS Software Assurance
- Self-Paced VA Fortify End User Training Materials Are Now Available
  Mike Boberski 9 19, 2016
  OIS Software Assurance
- Revised Guidance on Resolving Fortify Parsing and Syntax Scan Errors
  Matthew Condell 9 01, 2016
  OIS Software Assurance
- HPE Security Fortify Software Update (Patch) Version 16.11 Released
  Mike Boberski 8 01, 2016
  OIS Software Assurance
- Announcing Fortify Secure Coding Rulepacks Version 2016.2.0
  Mike Boberski 6 30, 2016

The Blog can be accessed HERE

Application Registration FAQ

How do I find out if my application has already been registered, to find its Application-ID?

To check if an application has been registered, you can search the internal link **here**.

Do I need to register my application?

All custom VA applications need to be registered with the VA Software Assurance Program Office, including those written in MUMPS or Delphi.[1] Registration is necessary in order to maintain an inventory of the total population of VA custom applications, by type and business line, to ensure application-level security considerations are taken into account when determining readiness and performance of a project.

> *[1] "Software Assurance Program Memorandum" (VAIQ #7477488), Stephen Warren, April 10, 2015.*

Can I reuse registrations (upload directory etc.) for more than one application?

No, registrations should not be reused for more than one application, and new components should build on prior submissions.

For example, let us say if there are applications or application components A and B, each of which is on a different development schedule and has a separate codebase.

One single registration could be used for,

- A, then
- A+B, as long as at this point A and B are then both submitted together going forward.

However if what is occurring though is something like code review validation submissions for,

- A, then
- B, i.e. A code/scans not submitted this time, then
- A+B, then
- A, i.e. B code/scans not submitted this time,
- Etc.

Then there is a problem, and A and B should be registered separately.

Secure Code Review FAQ

What are the terms of the VA license for Fortify?

All developers who contribute code to the source code base of each application to be scanned must be counted for license utilization, including the highest historical peak headcount, plus any additional security, test and management users. Contributing developers are then granted unlimited deployment to scanning servers, audit workbench clients, Visual Studio and Eclipse IDE plug-ins, and the collaboration portal for the source code base.

Note that under the license model, each individual person who is assigned a license is only counted once, no matter how many applications they contribute code to. Also, the license headcount can be reassigned for permanent transfers of licensed staff onto or off of projects, and for that matter in or out of VA. Licenses can be reassigned, as long as the person licensed is not contributing code for any other application at the VA.

Do I need to do code reviews?

Code reviews performed according to the **VA Secure Code Review SOP** are required for all VA software development, including those that are in sustainment with an ATO, with the exception of components that are written in MUMPS or Delphi. COTS software is also exempted from V&V secure code review validation A&A requirements.

Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [1] , and enforced as part of the ATO issuance process.[2]

Additionally, scanning source code to perform code review is a prerequisite to NSOC Web Application Security Assessments (WASAs) penetration tests [3]

> *[1] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.*
>
> *[2] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.*
>
> *[3] "WASA Questionnaire", question #2 "Technical / Testing Requirements Checklist: WASAs cannot be started until a V&V report is provided from the Software Assurance (SwA) team", VA NSOC intranet site.*

What if the code isn't MUMPS or Delphi but can't be scanned using Fortify, or perhaps some other extenuating circumstance?

In the event that the application is written in languages or environments not supported by Fortify, or perhaps some other extenuating circumstance, the reason/explanation will need to be documented in a Word document as to why code review cannot be done, whatever the reasoning is. Then title the document "Code Review" and upload to the RiskVision document tab (along with the failed code review validation report if an attempt had been made at the process).

The Certification Agent (CA) team will review this as part of the ATO review process and if they have questions as to the legitimacy of the reason, they will contact the VA Software Assurance Program Office. The CA team will then document this appropriately in the recommendations to the Authorizing Official (AO).

The CA will need this documentation evidence since there is no official exemption form or process.

When is guidance provided on this website effective as VA Secure Code Review SOP?

The guidance provided on this support site is effective immediately as VA Secure Code Review SOP. When new Fortify software and new Fortify rulepacks are released, the requirement to use these latest versions becomes effective in one week from the date of release.

My ATO / ATO with Conditions is at the program / system level. How many code reviews do I actually need?

You will need to do a code review, and have the results validated, for each individual application. The entire set of code review validation reports then needs to be checked into RiskVision when it comes time to enter into the A&A process.

How do code review activities fit into NSOC Web Application Security Assessment (WASA) activities?

A FAQ on the WASA activities including how code review activities fit in can be found **here**. (Note that access to the VA network is required to access the NSOC FAQ).

How can I install and configure the latest version of Fortify if the version listed in the TRM is not the current version?

The **Fortify SCA TRM entry** (internal link) Decision Constraint states "\[...] 3. The product must remain patched and operated in accordance with Federal and Department security and privacy policies and guidelines."

In general, the VA Software Assurance Program Office sets Federal and Department security and privacy policies and guidelines for using the Fortify software agency-wide.

To keep Fortify patched and operated according to VA Software Assurance Program Office policies and guidelines, you must keep up to date with the latest version of the Fortify software and the latest version of the Fortify rulepacks.

Newer versions of the Fortify software than those that may be listed on the TRM entry are patches to those older listed versions of the Fortify software and rulepacks.

How does Fortify licensing work in a Continuous Integration (CI) environment?

Generally, when you begin using your CI solution, it will need to be made sure that VA license terms are followed. In short in this configuration this means:

- The CI solution admins will need to request their own Fortify licenses
- Developers who use the solution once Fortify is part of it will need to first request Fortify per VA Software Assurance procedures before accessing the CI solution
- Testers, managers, or anyone who looks at .fpr files generated by the CI solution will additionally need to request their own Fortify licenses per VA Software Assurance procedures

Normal VA Software Assurance procedures for requesting the software is what will need to be done in each case.

- Then the VA Software Assurance license distribution email will become peoples' proof/ticket they've been properly provisioned access to the software per terms of the license. Also, **Here** is a sample email that you can use to check whether a user has already been provisioned the VA-licensed Fortify software.
- Then your procedures however they work can be followed as planned to allow access to CI solution functionality

How does Fortify licensing work when software is installed using enterprise systems management solutions like System Center Configuration Manager (SCCM)?

Generally, if Fortify software is to be pushed out in pre-built installation packages using a solution such as SCCM, it will need to be made sure that VA license terms are followed. In short in this configuration this means:

- The SCCM / SCCM-like solution admins will need to request their own Fortify licenses in order to build and maintain the Fortify package
- Developers who use the solution once Fortify is part of it will need to first request Fortify per VA Software Assurance procedures before the Fortify package is pushed to their machines

Normal VA Software Assurance procedures for requesting the software is what will need to be done in each case.

- Then the VA Software Assurance license distribution email will become peoples' proof/ticket they've been properly provisioned access to the software per terms of the license. Also, **Here** is a sample email that you can use to check whether a user has already been provisioned the VA-licensed Fortify software.
- Then your procedures however they work can be followed as planned to push the Fortify package to the user's machine

How often during development should I use Fortify?

Generally you should use it during development as early and often as possible, with the goal of not finding a lot of remaining problems when the time comes to do a final scan during the A&A process.

If you're doing continuous integration, you may want to include performing a scan in an automated fashion that way, rather than rely on individual developers to do scans on their own machines periodically.

But, however you use it though prior to the A&A process is up to you. We just review the final scan that is done during the attempt to get an ATO/TATO. See also VA ProPath BLD SDLC requirements.

What are "V&V Secure Code Reviews"?

Generally, VA Application Developers are responsible for performing their own secure code reviews of their applications both during development and the A&A process.

Secure code review Verification and Validations (V&V) are reviews of developer-performed scans to support obtaining an ATO or TATO that ensure VA requirements for performing secure code reviews have been met.

The overall process according to **VA Secure Code Review Standard Operating Procedures (SOP)** is as follows:

1. Developers first request Fortify, use it during component testing during development (and maintenance), and
2. Then prior to release, during the A&A process to obtain an ATO/TATO or per NSOC, developers do a final scan, and
3. It's at that point a V&V secure code review validation request package is submitted. The validation then checks that there are no remaining high or critical findings, and so on per the SOP.

What items are checked for during a V&V secure code review validation?

Specific items that are checked for include the following:

- Review developer-provided scan file for matching source code
- Review developer-provided scan file for scanning issues
- Review developer-provided scan file for residual findings
- Review developer-provided scan file for suppression of issues
- Review developer-provided custom rule files, if provided
- Perform additional supporting analysis, as needed

A technical note that provides additional details about steps that need to be performed by developers can be found **here**.

Examples of other common issues that should be addressed prior to a validation include:

- Hidden or Suppressed Issues: The **VA Secure Code Review Standard Operating Procedures (SOP)** require that issues be analyzed as "Not an Issue," with comments added explaining why the issues do not require code changes, instead of being hidden or suppressed.
- Out of Memory Issues: Fortify SCA can require intensive memory resources and out of memory exceptions are commonly reported, with the result that scans do not complete successfully and all potential issues in the application may not have been reported. See **this** technical note in the OIS SwA wiki for more information on how to correct out of memory issues.
- Other issues: Fortify may not have been configured properly to scan the application, resulting in incomplete scan results. Additional information on configuring Fortify correctly (SQL type, ASP or VBScript, ASP Precompilation errors, etc.) is available in the **Technical Notes** section of the OIS SwA wiki and in the Fortify SCA User Guide.

For more information, see section "Validation Strategy" in the "**Sample VA V&V Report Template**" that is posted in the "**Public Document Library**".

How do I ensure that Audit Workbench is displaying all issues detected by Fortify?

There are several steps to take to verify that Audit Workbench is displaying all the issues detected by the Fortify scan. First check that the Filter Set drop down box (located in the upper left hand corner of Audit Workbench) is set to "Security Auditor View." The other views show a subset of the results. Additionally, viewing hidden and suppressed issues should be enabled.

This is accomplished by selecting "Show Hidden Issues" and "Show Suppressed Issues" in the Options menu. Finally, check that the results reported by Fortify were not limited by any errors or warnings. This Technical Note (link to **How to view error messages reported by Fortify**) describes how to check for errors reported by the Fortify scan.

Also note that in Audit Workbench in the Audit Guide Wizard, you will need to select the “Show me all code quality issues” option. The other options may result in Fortify hiding issues which is prohibited by the SOP.

What does a V&V secure code review report look like?

The V&V secure code review report is a report that is suitable to use as a deliverable. To download a sample report template, click on “**Public Document Library**” in the sidebar on the left, then on the link for the "**Sample VA V&V Report Template**".

Why can't I use RBD's anymore?

As per version 4.0 of the OIS Field Security Service (FSS) Information Security Reference Guide, Risk based decisions (RBDs) will no longer be accepted. See also this VA Memo.

What sort of continuing professional education credits do I get for taking the VA Software Assurance Program Office courses?

It is at the present time up to organizations to which attendees belong to determine how or if VA Software Assurance Program Office training courses are recognized or credited. An email record of attendance will be provided to students upon completion of the course that may be helpful to use however might be appropriate by students.

How do I learn to use Fortify?

There are a number of options:

- To familiarize yourself with VA processes for using Fortify, you may wish to review the eLearning module **here**.
- To familiarize yourself with the Fortify tool in more detail, and also secure coding, we offer two developer courses; the current schedule for those is **here**.
- There is also a MyVEHU recorded eLearning module on the Fortify tool, information for that is **here**.

How can I import the validation report into my vulnerability management system?

In addition to a PDF report, a CSV-format file (comma-separated values file, file extension .csv) is also provided upon completion of a V&V secure code review validation, to facilitate importing results into a vulnerability management system in an automated fashion.

A separate .csv file is generated for each validation attempt. Notional examples are listed below. *Note that for amended reports, a new NSD ticket will need to be opened.*

- R1111111FY15-020150114-1.csv *(e.g. for initial validation)*
- R1111111FY15-020150114-2.csv *(e.g. for amended report issued same day)*
- R1111111FY15-020150120-1.csv *(e.g. for follow-on validation)*

The file format is as follows:

CSV File Format

```
NSD-Ticket,FISMA-System,Application-Name,A
pplication-Version,Validation-Date,Result,
Severity,CWE-ID,CWE-Title,Count
```

Notional file example for a pass/fail validation result:

CSV File Example

```
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,Pass,Critical,N/A,N/A,0
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,Pass,High,N/A,N/A,0
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,N/A,Medium,N/A,N/A,0
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,POAM Required,Low,CWE-570,Dead
Code: Expression is Always false,2
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,POAM Required,Low,CWE-571,Dead
Code: Expression is Always true,5
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,POAM
Required,Low,CWE-615,Password Management:
Password in Comment,2
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,POAM Required,Low,CWE-391,Poor
Error Handling: Empty Catch Block,7
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,Pass,Scan Issues,N/A,N/A,0
```

Notional file example for an incomplete validation result, where blocking issues were encountered during a validation attempt and thus any current scan results should not be relied upon, and another validation attempt is required in order to even get to the point where pass/fail can be determined:

CSV File Example

```
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,Unknown,Critical,N/A,N/A,-1
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114, Unknown,High,N/A,N/A,-1
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114, Unknown,Medium,N/A,N/A,-1
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114, Unknown,Low, N/A,N/A,-1
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,Fail,Scan Issues,N/A,Some
blocking problem,3
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,Fail,Scan Issues,N/A,Some other
blocking problem,2000
R1111111FY15,SomeSystem,SomeApplication,3.
1,20150114,Fail,Scan Issues,N/A,Etc etc,54
```

Additional details:

- **NSD-Ticket** – This is the NSD ticket that corresponds to the V&V secure code review validation request. *Note that follow-on reviews will be provided in separate files.*
- **FISMA-System** – This is the developer-provided FISMA system name that corresponds/contains the application.
- **Application-Name** – This is the name of the application for which Fortify scanning/auditing was performed.
- **Application-Version** – This is the version of the application for which Fortify scanning/auditing was performed.
- **Validation-Date** – This is the date the VA Software Assurance Program Office completed the validation.
- **Result** – This is the result of the V&V secure code review validation (Pass, Fail, Incomplete)
- **Severity** – These are the severities as they appear in VA Software Assurance Program Office reports (Critical, High, Medium, Low, Unresolved Scan Issues). *Note that Additional FIndings are rolled into corresponding severities.*
- **CWE-ID** – These are the CWE numbers as they appear in VA Software Assurance Program Office reports (MITRE-defined CWE, or N/A for e.g. Fortify scan issues). *Note that if no CWE, will be "N/A"; also note that if multiple CWE, then separated by spaces e.g. "CWE-xx CWE-yy"*
- **CWE-Title** – These are the CWE titles as they appear in VA Software Assurance Program Office reports (MITRE-defined CWE, or N/A for e.g. Fortify scan issues)
- **Count** – These are the number of instances of each CWE as they appear in VA Software Assurance Program Office reports. *Note that these numbers are the RBD-adjusted numbers (or e.g. a Fortify bug-adjusted number) if applicable.*

When registering my application, when determining line of business for an application, should the VA consumer organization or the VA development organization be specified?

Generally we want to be as specific as possible. So if you know the consumer should go with that. Ideally for example no one should just use the top-level VHA/VBA/NCA buckets.

Example: Let us say that PD is the developer of an Application X and an Application Y. Application X is a custom application that provides all of some service type for the entire VA. Application Y is the custom application that is used by a very specific VA line of business that is the consumer of the application from PD's perspective.

In this example, Application X should be mapped to PD, and Application Y should be mapped to the very specific VA line of business that is the consumer of the application from PD's perspective.

Deprecated - What if my version of Xcode is not supported by Fortify?

Below are the A&A code review validation procedures if the version of Xcode is not supported by the current version of Fortify at the time of the V&V secure code review validation request. For example, if new iOS apps uploaded to the App Store are required by Apple to use a newer version than Fortify currently supports. Note that this is the only circumstance that Clang may be substituted for Fortify for scanning projects built using Xcode in order to meet A&A requirements for code review.

If Xcode supported by Fortify	If Xcode not supported by Fortify	Notes
Use Fortify	Use Clang	Clang is built into Xcode. The options below should be used. If an option is not specified below, the developer may choose what is most appropriate for their app.

- Apple LLVM - Warnings - All languages
  - Implicit Boolean Conversions: Yes
  - Implicit Constant Conversions: Yes
  - Implicit Conversion to 32 Bit Type: Yes
  - Implicit Enum Conversions: Yes
  - Implicit Integer to Pointer Conversions: Yes
  - Implicit Signedness Conversions: Yes
  - Unreachable Code: Yes
  - Unused Functions: Yes
- Static Analyzer - Analysis Policy Settings:
  - Mode of Analysis for 'Analyze': Deep
  - Mode of Analysis for 'Build': Deep
- Static Analyzer - Generic Issues Settings:
  - Dead Stores: Yes
  - Improper Memory Management: Yes
  - Misuse of Grand Central Dispatch: Yes

- Static Analyzer - Issues - Objective-C Settings:
  - '@synchronized with nil mutex: Yes
  - Improper Handling of CFError and NSError: Yes
  - Method Signatures Mismatch: Yes
  - Misuse of Collections API: Yes
  - Unused Ivars: Yes
  - Violation of 'self = \[super init]' Rule: Yes
  - Violation of Reference Counting Rules: Yes
- Static Analyzer - Issues - Security Settings:
  - Floating Point Value used as Loop Counter: Yes
  - Misuse of Keychain Services API: Yes
  - Unchecked Return Values: Yes
  - Use of 'getpw', 'gets' (buffer overflow): Yes
  - Use of 'rand' Functions: Yes
  - Use of 'strcpy' and 'strcat': Yes

Pass criteria as per the SOP: • 0 critical • 0 high • 0 scan issues	Pass criteria per this guidance: • 0 findings from security checkers (i.e. Clang rulesets) • 0 scan issues	All Clang security checker (i.e. security.* checks, which are static analysis tool rulesets) findings must be fixed. Reference: http://clang-analyzer.llvm.org/available_checks.html#security_checkers The following Clang security checker findings which check for insecure API usage and perform checks based on the CERT Secure Coding Standards will be mapped to high severity: • security.* checks Remaining Clang security checker findings will be mapped to low severity. And, if there are Clang scan issues (i.e. errors reported from the command line invocation of Clang), must be fixed.
Validation requests require: • Fortify scan files • Zip of source code • See FAQ for NSD ticket etc.	Validation requests require: • Zip of Clang HTML scan results • Document with capture of command-line invocation of Clang • Zip of source code • Readme with the exact version of Xcode that was used (e.g. 6.1) • See FAQ for NSD ticket etc.	Validation request procedures per the norm should otherwise be followed (e.g. requesting upload directory etc.). Document with capture of command-line invocation of Clang must be provided so that it can be determined if there were any errors not addressed when performing the scan using Clang.
Validation false positives require: • Annotating Fortify scan with explanation	Validation false positives require: • Providing readme as part of validation submission package with explanation referencing Clang HTML scan results	Explanations need to be per instance, for security findings that are not fixed.

Secure Design Review FAQ